UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/762,555	04/10/2001	Lothrop Mittenthal	TET-1668/980	6718

7590 05/06/2004

Robert A Muha
Kirkpatrick & Lockhart
Henry W Oliver Building
535 Smithfield Street
Pittsburgh, PA 15222-2312

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 05/06/2004

11

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/762,555	Applicant(s) MITTENTHAL, LOTHROP
	Examiner Christian La Forgia	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed on 09 February 2004 is noted and made of record.

2. Claims 1-22 are presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1-22 have been considered but are moot in view of the new ground(s) of rejection.

4. See further rejections that follow.

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,182,216 to Luyster, hereinafter Luyster, in view of U.S. Patent No. 5,317,639 to Mittenthal, hereinafter Mittenthal.

7. As per claim 1, Luyster teaches method of deterministically generating maximal nonlinear block substitution tables for a predetermined block size, comprising:

selecting a first generating function (Figures 1 [blocks k1, k2], 2 [block key1, key 2], 5 [blocks 92, 100g], 11; column 38, lines 24-36; column 51, lines 19-67);

selecting a second generating function (Figures 5 [blocks 94, 100h], 11; column 38, lines 24-36; column 51, lines 19-67);

selecting first and second sets of complete linearly independent numbers (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7

[blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

calculating first and second linear functions from the generating functions and the sets of linearly independent numbers (Figure 1 [blocks 16, 18], 3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60).

8. Luyster discloses combining first and second linear functions to produce a nonlinear block substitution table, or s-box, as evident by at least the Abstract.

9. Luyster discloses the claimed invention except for the use of linear orthomorphisms, thereby failing to create maximal nonlinear block substitution tables by combining the linear orthomorphisms. Mittenthal discloses using nonlinear orthomorphisms to create maximal nonlinear block substitution tables. It would have been obvious to one having ordinary skill in the art at the time the invention was made to use linear orthomorphic functions to generate a nonlinear block substitution table as taught by Mittenthal, since Mittenthal discloses at column 2, lines 39-43 that such a modification would make cryptanalysis more difficult. Furthermore, Mittenthal discloses in column 19, lines 26-32 that generating nonlinear orthomorphisms involves routine skill in the art.

10. Regarding claim 2, Luyster teaches wherein selecting a first generating function includes selecting a first primitive generating function (Figure 6; column 37, lines 55 to column 38, lines 23).

11. Regarding claim 3, Luyster teaches wherein selecting a first generating function includes selecting a first nonprimitive generating function (Figure 6; column 37, lines 28-45).

12. Regarding claim 4, Luyster teaches wherein selecting a second generating function includes selecting a second primitive generating function (Figure 6; column 37, lines 55 to column 38, lines 23).

13. Regarding claim 5, Luyster teaches wherein selecting a second generating function includes selecting a second nonprimitive generating function (Figure 6; column 37, lines 28-45).

14. With regards to claim 6, Luyster teaches wherein selecting a second non-primitive generating function includes selecting a second non-primitive generating function having a cycle pattern that is identical to a cycle pattern of the first generating function (column 37, lines 18-45).

15. Regarding claim 7, Luyster teaches wherein calculating first and second linear orthomorphisms includes calculating first and second maximal linear orthomorphisms from the generating functions and the sets of linearly independent numbers (Figure 1 [blocks 16, 18], 3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60).

16. Regarding claim 8, Luyster teaches further comprising rotating the second linear orthomorphism (column 37, lines 37-45). It would have been obvious to one of ordinary skill in the art at the time the invention was made to rotate the second linear orthomorphism. One would be motivated to adopt this technique because it is fast, simple, and add more security.

17. With regards to claim 9, Luyster teaches wherein rotating the second linear orthomorphism includes rotating corresponding cycles of the second linear orthomorphism (column 37, lines 37-45).

18. Regarding claim 10, Luyster teaches wherein selecting a second generating function includes selecting a second generating function which is a complement of the first generating function (column 38, lines 5-36; column 39, line 60 to column 40, lines 28).

19. Regarding claim 11, Luyster teaches wherein selecting a second generating function includes selecting a second generating function which is any generating function that is not identical to the first generating function and has a cycle structure which matches a cycle structure of the first generating function (column 38, lines 5-36; column 39, line 60 to column 40, lines 28).

20. Regarding claim 12, Luyster teaches wherein selecting first and second sets of linearly independent numbers includes selecting a second set of linearly independent numbers that is identical to the first set of linearly independent numbers (column 39, lines 17-28).

21. Regarding claim 13, Luyster teaches wherein selecting first and second sets of linearly independent numbers includes selecting a second set of linearly independent numbers that is not identical to the first set of linearly independent numbers (column 39, lines 17-28).

22. Regarding claim 14, Luyster teaches further comprising determining whether all cycles of the first and second linear orthomorphisms are self-contained (column 23, line 50 to column 24, line 27).

23. With regards to claim 15, Luyster teaches further comprising selecting pairs of cycles from the first and second linear orthomorphisms to produce a mapping for which $N(x,y)!=0$ for all pairs of numbers from different cycles (Figure 12; column 33, line 37 to column 34, line 36).

24. As per claim 16, Luyster teaches a computer-implemented method for deterministically generating maximal nonlinear block substitution tables from binary data, comprising:

selecting a first set of a plurality of complete linearly independent numbers from the binary data (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

selecting a second set of a plurality of complete linearly independent numbers from the binary data (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6

[blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

generating plurality of linear functions using first and second recursive generating function and the first and second sets of linearly independent numbers (Figure 1 [blocks 16, 18], 3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60).

25. Luyster discloses combining first and second linear functions to produce a nonlinear block substitution table, or s-box, as evident by at least the Abstract.

26. Luyster discloses the claimed invention except for the use of linear orthomorphisms, thereby failing to set a maximal nonlinear block substitution tables based on the combination of the linear orthomorphisms. Mittenthal discloses using nonlinear orthomorphisms to create maximal nonlinear block substitution tables. It would have been obvious to one having ordinary skill in the art at the time the invention was made to use linear orthomorphic functions to generate a nonlinear block substitution table as taught by Mittenthal, since Mittenthal discloses at column 2, lines 39-43 that such a modification would make cryptanalysis more difficult. Furthermore, Mittenthal discloses in column 19, lines 26-32 that generating nonlinear orthomorphisms involves routine skill in the art.

27. Regarding claims 17 and 19, Luyster teaches wherein the second generating function is a complement of the first generating function (column 39, lines 17-28). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the second function be a complement of the first function. It merely be a fact of reversing parts to ensure

different keys between the two halves. See MPEP § 2144.04. See also *In re Gazda*, 219 F.2d 449, 452, 104 USPQ 400, 402 (CCPA 1955).

28. As per claim 18, Luyster teaches a computer-implemented method for deterministically generating maximal nonlinear block substitution tables from binary data, comprising:

selecting a first set of a plurality of complete linearly independent numbers from the binary data (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

selecting a second set of a plurality of complete linearly independent numbers from the binary data (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28).

29. Luyster does not teach recursively applying a first generating function to the first set of linearly independent numbers to create a major cycle of a first orthomorphism; generating a plurality of cycles of the first orthomorphism; recursively applying a second generating function to the second set of linearly independent numbers to create a major cycle of a second orthomorphism; generating a plurality of cycles of the second orthomorphism; and setting the maximal nonlinear substitution tables by combining the linear orthomorphisms, the substitution tables for us in encrypting clear text messages which are in the form of an ordering of binary numbers.

30. Luyster discloses the claimed invention except for the use of linear orthomorphisms, thereby failing to set a maximal nonlinear block substitution tables based on the combination of the linear orthomorphisms. Mittenthal discloses using nonlinear orthomorphisms to create maximal nonlinear block substitution tables. It would have been obvious to one having ordinary skill in the art at the time the invention was made to use linear orthomorphic functions to generate a nonlinear block substitution table as taught by Mittenthal, since Mittenthal discloses at column 2, lines 39-43 that such a modification would make cryptanalysis more difficult. Furthermore, Mittenthal discloses in column 19, lines 26-32 that generating nonlinear orthomorphisms involves routine skill in the art.

31. As per claims 20, 21 and 22, Luyster teaches a system, comprising:

a communications link (column 56, line 60 to column 57, line 12);

a first computer in communication with the communications link (column 56, line 60 to column 57, line 12); and

a second computer in communications with the communications link (column 56, line 60 to column 57, line 12), the second computer having an ordered read set of data and instructions stored thereon which, when executed by the second computer cause the second computer to perform the steps of:

selecting a first generating function (Figures 1 [blocks k1, k2], 2 [block key1, key 2], 5 [blocks 92, 100g], 11; column 38, lines 24-36; column 51, lines 19-67);

selecting a second generating function (Figures 5 [blocks 94, 100h], 11; column 38, lines 24-36; column 51, lines 19-67);

selecting first and second sets of complete linearly independent numbers (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

calculating first and second linear functions from the generating functions and the sets of linearly independent numbers (Figure 1 [blocks 16, 18], 3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60).

32. Luyster discloses combining first and second linear functions to produce a nonlinear block substitution table, or s-box, as evident by at least the Abstract.

33. Luyster discloses the claimed invention except for the use of linear orthomorphisms, thereby failing to create maximal nonlinear block substitution tables by combining the linear orthomorphisms. Mittenthal discloses using nonlinear orthomorphisms to create maximal nonlinear block substitution tables. It would have been obvious to one having ordinary skill in the art at the time the invention was made to use linear orthomorphic functions to generate a nonlinear block substitution table as taught by Mittenthal, since Mittenthal discloses at column 2, lines 39-43 that such a modification would make cryptanalysis more difficult. Furthermore, Mittenthal discloses in column 19, lines 26-32 that generating nonlinear orthomorphisms involves routine skill in the art.

Conclusion

34. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

35. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

36. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100